U.S. DEPARTMENT OF COMMERCE PATENT & TRADEMARK OFFICE

B/O Form PTO-1390 **Transmittal Letter to the United States Designated/Elected Office (DO/EO/US) Concerning a Filing Under *35 USC 371***		*Attorney's Docket Number* JEK/Vater
		U.S. Application Number (if known) 09/763621
International Application Number PCT/EP99/06580	*International Filing Date* 07 September 1999	*Priority Date Claimed* 11 September 1998
Title of Invention ACCESS-PROTECTED DATA CARRIER		
Applicant(s) for DO/EO/US Harald VATER et al.		

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items under *35 USC 371*:

1. ☒ This is a **FIRST** submission of items concerning a filing under *35 USC 371*.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under *35 USC 371*.
3. ☒ This express request to begin national examination procedures *(35 USC 371(f))* at any time rather than delay examination until the expiration of the applicable time limit set in *35 USC 371(b)* and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed *35 USC 371(c)(2)*.
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English *(35 USC 371(c)(2))*.
7. ☒ Amendments to the claims of the International Application under PCT Article 19 *(35 USC 371(c)(3))*
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 *(35 USC 371(c)(3))*.
9. ☒ An oath or declaration of the inventor(s) *(35 USC 371(c)(4))*. (☐ Executed ☒ Unexecuted)
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 *(35 USC 371(c)(5))*.

Items 11 to 16 below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under *37 CFR 1.97* and *1.98*.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with *37 CFR 3.28* and *3.31* is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: 2 sheets of formal drawings

Application Number (if Known) 09/763621	*International Application Number* PCT/EP99/06580	*Attorney's Docket Number* JEK/Vater

	Calculations	PTO USE ONLY
17. The following fees are submitted: **Basic National Fee *(37 CFR 1.492(a)(1)-(5))*:** ☒ Search report has been prepared by the EPO or JPO . . . . . $840.00 ☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* . . . . . $690.00 ☐ No International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* but International Search Fee paid to USPTO *(37 CFR 1.445(a)(2))* . . . . . $710.00 ☐ Neither International Preliminary Examination Fee *(37 CFR 1.482)* nor International Search Fee *(37 CFR 1.445(a)(2))* paid to USPTO . . . . . $1000.00 ☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT	**$ 840.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(e))*.		

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total Claims	18 -20 =		× $18.00		
Independent Claims	2 -3 =		× $80.00		
Multiple Dependent Claims (if applicable)			+ $270.00		
TOTAL OF ABOVE CALCULATIONS				**$ 840.00**	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity Statements must also be filed (Note *37 CFR 1.9, 1.27, 1.28)*					
SUBTOTAL				**$ 840.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(f))*.					
TOTAL NATIONAL FEE				**$ 840.00**	
Fee for recording the enclosed assignment *(37 CFR 1.21(h))*. The assignment must be accompanied by an appropriate cover sheet *(37 CFR 3.28, 3.31)*. **$40.00** per property.					
TOTAL FEES ENCLOSED				**$ 840.00**	
Amount to be: Refunded:					
Charged:					

a. ☒ A check in the amount of **$840.00** to cover the fees is enclosed.

b. ☐ Please charge my **Deposit Account Number 02-0200** in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to **Deposit Account Number 02-0200**. A duplicate copy of this sheet is enclosed.

Note: Where an appropriate time limit under *37 CFR 1.494* or *1.495* has not been met, a petition to revive *(37 CFR 1.137(a) or (b))* must be filed and granted to restore the application to pending status.

BACON & THOMAS, PLLC
625 SLATERS LANE - FOURTH FLOOR
ALEXANDRIA, VIRGINIA 223124-1176
(703) 683-0500

DATE: 05 March 2001

Respectfully submitted,

J. ERNEST KENNEY
Attorney for Applicant
Registration Number: 19,179

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

International Patent Application
No. PCT/EP99/06580

PCT/DO/EO/US

International Filing Date: 07 September 1999

Applicant: Harald VATER et al.

For: ACCESS-PROTECTED DATA CARRIER

PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

This paper accompanies documents submitted to establish the U.S. national stage of the above-identified international patent application.

Before calculation of the filing fee and before examination, kindly amend the claims as follows:

IN THE CLAIMS:

Please amend claims 3, 4, 6, 7, 11, 12, 15, 16 and 18 as shown on the appended APPENDIX OF CLAIMS. For the convenience of the Examiner, all claims pending in this application are shown on the Appendix of Claims. In addition, an Appendix of Marked Up Claims showing the amendments is provided herewith.

REMARKS

All rights are reserved to the original claimed subject matter. The claims have been amended to reduce the filing fees and to correct any improper multiple dependent claims. Examination of the application as amended is respectfully requested.

Respectfully submitted,
BACON & THOMAS, PLLC

J. ERNEST KENNEY
Attorney for Applicant
Registration Number 19,179

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314
Telephone: (703) 683-0500
Facsimile: (703) 683-1080

Date: March 4, 2001
S:\Producer\jek\VATER - pct06580\preliminary amendment.wpd

APPENDIX OF CLAIMS

1. A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation *(h)*, the execution of the operation *(h)* requiring input data *(x)* and the execution of the operation *(h)* generating output data *(y)*, characterized in that

the operation *(h)* is disguised before its execution,

the disguised operation (h_{R1}) is executed with disguised input data $(x \otimes R_1)$, and

the disguising of the operation *(h)* and the input data *(x)* is coordinated such that the execution of the disguised operation (h_{R1}) with disguised input data $(x \otimes R_1)$ yields output data *(y)* identical with the output data *(y)* determined upon execution of the undisguised operation *(h)* with undisguised input data *(x)*.

2. A data carrier according to claim 1, characterized in that at least one random number (R_1) enters into the determination of the disguised operation (h_{R1}) and the disguised input data $(x \otimes R_1)$.

3(amended). A data carrier according to claim 1, characterized in that the determination of the disguised operation (h_{R1}) and the disguised input data $(x \otimes R_1)$ is effected with the aid of EXOR operations.

4(amended). A data carrier according to claim 1, characterized in that the disguised operation (h_{R1}) is permanently stored in the data carrier in advance.

5. A data carrier according to claim 4, characterized in that at least two disguised operations $(h_{R1}, h_{R1'})$ are permanently stored in the data carrier in advance

and one of the stored disguised operations (h_{R1}, h_{R1}) is selected randomly when a disguised operation is to be executed.

6(amended). A data carrier according to claim 1, characterized in that the disguised operation (h_{R1}) is recalculated before its execution and the at least one random number (R_1) is redetermined for said calculation.

7(amended). A data carrier according to claim 1, characterized in that the operation *(h)* is realized by a table stored in the data carrier which establishes an association between the input data *(x)* and the output data *(y)*.

8. A data carrier according to claim 7, characterized in that the disguising of the input data *(x)* contained in the table is effected by combination with the at least one random number (R_1).

9. A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation *(h)*, the execution of the operation *(h)* requiring input data *(x)* and the execution of the operation *(h)* generating output data *(y)*, characterized in that

the operation *(h)* is disguised before its execution,

the disguised operation (h_{R1}) is executed with disguised input data $(x \otimes R_1)$,

the disguising of the operation *(h)* and the input data *(x)* is coordinated such that the execution of the disguised operation (h_{R1R2}) with disguised input data $(x \otimes R_1)$ yields output data $(y \otimes R_2)$ which are disguised relative to the output data *(y)* determined upon execution of the undisguised operation *(h)* with undisguised input data (x), and

the undisguised output data *(y)* can be determined from the disguised output data *($y \otimes R_2$)* with the aid of data *(R_2)* used for disguising the operation *(h)*.

10. A data carrier according to claim 9, characterized in that at least one random number (R_1) enters into the determination of the disguised input data *($x \otimes R_1$)* and at least two random numbers *(R_1, R_2)* enter into the determination of the disguised operations *(h_{R1R2})*.

11(amended). A data carrier according to claim 9, characterized in that the determination of the disguised operation *(h_{R1R2})* and the disguised input data *($x \otimes R_1$)* is effected with the aid of EXOR operations.

12(amended). A data carrier according to claim 9, characterized in that the disguised operation *(h_{R1R2})* is permanently stored in the data carrier in advance.

13. A data carrier according to claim 12, characterized in that at least two disguised operations *(h_{R1R2}, $h_{R1'R2'}$)* are permanently stored in the data carrier in advance and one of the stored disguised operations *(h_{R1R2}, $h_{R1'R2'}$)* is selected randomly when a disguised operation is to be executed.

14. A data carrier according to claim 13, characterized in that the random numbers *(R_1, R_2)* for determining the first disguised operation *(h_{R1R2})* are inverse to the random numbers *(R_1', R_2')* for determining the second disguised operation *($h_{R1'R2'}$)* with respect to the combination used for determining the disguised operations *(h_{R1R2}, $h_{R1'R2'}$)*.

15(amended). A data carrier according to claim 9, characterized in that the disguised operation *(h_{R1R2})* is recalculated before its execution and the random numbers *(R_1, R_2)* are redetermined for said calculation.

16(amended). A data carrier according to claim 9, characterized in that the operation *(h)* is realized by a table stored in the data carrier which establishes an association between the input data *(x)* and the output data *(y)*.

17. A data carrier according to claim 16, characterized in that the disguising of the input data *(x)* contained in the table is effected by combination with the at least one random number (R_1) and the disguising of the output data *(y)* contained in the table is effected by combination with the at least one further random number (R_2).

18(amended). A data carrier according to claim 1, characterized in that the operation *(h)* is a nonlinear operation with respect to the combination used for disguising the operation *(h)*.

S:\Producer\jek\VATER - pct06580\appendix of claims wpd

Appendix of marked-up claims

09/763621
PCT/EP99/06580
JEK/VPTER
528 Rec'd PCT/PTO 05 MAR 2001

Patent claims

1. A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that
   - the operation (h) is disguised before its execution,
   - the disguised operation (h_{R1}) is executed with disguised input data ($x \otimes R_1$), and
   - the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h_{R1}) with disguised input data ($x \otimes R_1$) yields output data (y) identical with the output data (y) determined upon execution of the undisguised operation (h) with undisguised input data (x).
2. A data carrier according to claim 1, characterized in that at least one random number (R_1) enters into the determination of the disguised operation (h_{R1}) and the disguised input data ($x \otimes R_1$).
3. A data carrier according to [either] Claim 1 [of the above claims] characterized in that the determination of the disguised operation (h_{R1}) and the disguised input data ($x \otimes R_1$) is effected with the aid of EXOR operations.
4. A data carrier according to [any] Claim 1 [of the above claims] characterized in that the disguised operation (h_{R1}) is permanently stored in the data carrier in advance.
5. A data carrier according to claim 4, characterized in that at least two disguised operations (h_{R1}, $h_{R1'}$) are permanently stored in the data carrier in advance and one of the stored disguised operations (h_{R1}, $h_{R1'}$) is selected randomly when a disguised operation is to be executed.
6. A data carrier according to [any] Claim 1 [of claims 1 to 3] characterized in that the disguised operation (h_{R1}) is recalculated before its execution and the at least one random number (R_1) is redetermined for said calculation.

7. A data carrier according to any of the above claims, characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y).

8. A data carrier according to claim 7, characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1).

9. A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that
   - the operation (h) is disguised before its execution,
   - the disguised operation (h_{R1}) is executed with disguised input data ($x \otimes R_1$),
   - the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h_{R1R2}) with disguised input data ($x \otimes R_1$) yields output data ($y \otimes R_2$) which are disguised relative to the output data (y) determined upon execution of the undisguised operation (h) with undisguised input data (x), and
   - the undisguised output data (y) can be determined from the disguised output data ($y \otimes R_2$) with the aid of data (R_2) used for disguising the operation (h).

10. A data carrier according to claim 9, characterized in that at least one random number (R_1) enters into the determination of the disguised input data ($x \otimes R_1$) and at least two random numbers (R_1, R_2) enter into the determination of the disguised operations (h_{R1R2}).

11. A data carrier according to either of claims 9 and 10, characterized in that the determination of the disguised operation (h_{R1R2}) and the disguised input data ($x \otimes R_1$) is effected with the aid of EXOR operations.

12. A data carrier according to any of claims 9 to 11, characterized in that the disguised operation (h_{R1R2}) is permanently stored in the data carrier in advance.

13. A data carrier according to claim 12, characterized in that at least two disguised operations (h_{R1R2}, $h_{R1'R2'}$) are permanently stored in the data carrier in advance and one of the stored disguised operations (h_{R1R2}, $h_{R1'R2'}$) is selected randomly when a disguised operation is to be executed.

14. A data carrier according to claim 13, characterized in that the random numbers (R_1, R_2) for determining the first disguised operation (h_{R1R2}) are inverse to the random numbers (R_1', R_2') for determining the second disguised operation ($h_{R1'R2'}$) with respect to the combination used for determining the disguised operations (h_{R1R2}, $h_{R1'R2'}$).

15. A data carrier according to any of claims 9 to 11, characterized in that the disguised operation (h_{R1R2}) is recalculated before its execution and the random numbers (R_1, R_2) are redetermined for said calculation.

16. A data carrier according to any of claims 9 to 15, characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y).

17. A data carrier according to claim 16, characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1) and the disguising of the output data (y) contained in the table is effected by combination with the at least one further random number (R_2).

18. A data carrier according to any of the above claims, characterized in that the operation (h) is a nonlinear operation with respect to the combination used for disguising the operation (h).

Access-protected data carrier

This invention relates to a data carrier having a semiconductor chip in which secret data are stored. The invention relates in particular to a smart card.

Data carriers containing chips are used in a great number of different applications, for example for performing monetary transactions, paying for goods or services, or as an identification means for access or admission controls. In all said applications the data carrier chip normally processes secret data which must be protected from access by unauthorized third parties. Said protection is ensured by, among other things, giving the inner structures of the chip very small dimensions so that it is very difficult to access said structures with the aim of spying out data processed in said structures. In order to impede access further, one can embed the chip in a very firmly adhering compound whose forcible removal destroys the semiconductor plate or at least the secret data stored therein. It is also possible to provide the semiconductor plate during its production with a protective layer which cannot be removed without destroying the semiconductor plate.

With corresponding technical equipment, which is extremely expensive but nevertheless fundamentally available, an attacker could possibly succeed in exposing and examining the inner structure of the chip. Exposure could be effected for example by special etching methods or a suitable grinding process. The thus exposed structures of the chip, such as conductive paths, could be contacted with microprobes or examined by other methods to determine the signal patterns in said structures. Subsequently, one could attempt to determine from the detected signals secret data of the data carrier, such as secret keys, in order to use them for purposes of manipulation. One could likewise attempt to selectively influence the signal patterns in the exposed structures via the microprobes.

The invention is based on the problem of protecting secret data present in the chip of a data carrier from unauthorized access.

This problem is solved by the feature combinations of claims 1 and 9.

The inventive solution does not aim, like the prior art, at preventing exposure of the internal structures of the chip and the mounting of microprobes. Instead

measures are taken to make it difficult for a potential attacker to infer secret information from any signal patterns intercepted. Said measures consist according to the invention in manipulating security-relevant operations so that the secret data used in performing said security-relevant operations cannot be determined without including further secret information. For this purpose the security-relevant operations are disguised or falsified with the aid of suitable functions before execution. In order to impede or even prevent in particular a statistical evaluation in case of multiple execution of the security-relevant operations, a random component enters into the disguising function. As a result, an attacker cannot determine the secret data from any data streams intercepted.

The security-relevant operation will be represented in the following by function h mapping input data x on output data y, i.e. $y = h(x)$. To prevent secret input data x from being spied out the invention provides for disguised function h_{R1R2} to be determined, so that the following holds:

$$y \otimes R_2 = h_{R1R2}\,(x \otimes R_1).$$

The security-relevant operation is now performed by means of disguised function h_{R1R2} whose input data are not authentic secret data x but disguised secret data $x \otimes R_1$ generated by combining authentic secret data x with random number R_1. Without knowledge of random number R_1 one cannot determine authentic secret data x from disguised secret data $x \otimes R_1$. As a result of applying disguised function h_{R1R2} to disguised secret data $x \otimes R_1$ one obtains disguised output data $y \otimes R_2$. From disguised output data $y \otimes R_2$ one can determine output data y by suitable combination. Before each new execution of the security-relevant function one can preset new random numbers R_1 and R_2 from which new disguised function h_{R1R2} is determined in each case. Alternatively, a plurality of disguised functions h_{R1R2} can be permanently stored, one of which is selected randomly before execution of the security-relevant operation. It is especially advantageous to use two functions h_{R1R2} and $h_{R1'R2'}$, random numbers R_1' and R_2' being the inverse values of random numbers R_1 and R_2 with respect to the type of combination selected for disguising. In a further variant, random numbers R_1 and R_2 can also be identical. In particular, random num-

bers R_1 and R_2 can be selected statistically independently so that there is no correlation between input and output data which can be used for an attack.

If further operations are executed before or after security-relevant operation h in question here, random numbers R_1 and R_2 can also be used for disguising the data processed with the further operations.

The inventive solution can be used especially advantageously for security-relevant operations containing nonlinear functions. With nonlinear functions one cannot apply known protective measures based on disguising the secret data before execution of the functions. Known protective measures presuppose that the functions are linear with respect to the disguising operations so that disguising can be undone after execution of the functions. In the inventive solution, however, not only the secret data are falsified or disguised but also the security-relevant operations processing the secret data. The disguising of the secret data and the security-relevant operations is coordinated such that the authentic secret data can be derived from the disguised secret data after execution of the security-relevant operations. Coordination between disguising of the secret data and the security-relevant operations can be realized especially simply if the security-relevant operations are realized in the form of tables, so-called lookup tables. In the stated tables each input value x has output value y associated therewith. The functions realized by the tables are executed by looking up output values y belonging to particular input values x.

The invention will be explained below with reference to the embodiments shown in the figures, in which:

Fig. 1 shows a smart card in a top view,

Fig. 2 shows a greatly enlarged detail of the chip of the smart card shown in Fig. 1 in a top view,

Figs. 3a, 3b, 3c and 3d show representations of lookup tables.

Fig. 1 shows smart card 1 as an example of the data carrier. Smart card 1 is composed of card body 2 and chip module 3 set in a specially provided gap in card body 2. Essential components of chip module 3 are contact surfaces 4 for producing an electric connection with an external device, and chip 5 electrically connected with contact surfaces 4. As an alternative or in addition to contact surfaces 4, a coil not

shown in Fig. 1 or other transfer means can be present for producing a communication link between chip 5 and an external device.

Fig. 2 shows a greatly enlarged detail of chip 5 from Fig. 1 in a top view. The special feature of Fig. 2 is that it shows the active surface of chip 5, i.e. it does not show all layers generally protecting the active layer of chip 5. In order to obtain information about the signal patterns in the interior of the chip one can for example contact exposed structures 6 with microprobes. Microprobes are very thin needles which are brought in electric contact with exposed structures 6, for example conductive paths, by means of a precision positioning device. The signal patterns picked up by the microprobes are processed with suitable measuring and evaluation devices with the aim of inferring secret data of the chip.

The invention makes it very difficult or even impossible for an attacker to gain access to in particular secret data of the chip even if he has managed to remove the protective layer of chip 5 without destroying the circuit and to contact exposed structures 6 of chip 5 with microprobes or intercept them in some other way. The invention is of course also effective if an attacker gains access to the signal patterns of chip 5 in another way.

Figures 3a, 3b, 3c and 3d show simple examples of lookup tables in which the input and output data each have a length of 2 bits. All table values are represented as binary data. The first line states input data x, and the second line output data y associated therewith in the particular column.

Figure 3a shows a lookup table for undisguised function h. Figure 3a indicates that input value $x = 00$ has output value $h(x) = 01$ associated therewith, input value 01 output value 11, input value 10 output value 10, and input value 11 output value 00. The lookup table according to Figure 3a represents nonlinear function h which is to be executed within the framework of a security-relevant operation. According to the invention, however, one does not use the lookup table shown in Figure 3a itself in executing the security-relevant operation, but derives a disguised lookup table from said lookup table according to Figures 3b, 3c and 3d.

Figure 3b shows an intermediate step in determining the disguised lookup table. The lookup table according to Figure 3b was generated from the lookup table

according to Figure 3a by EXORing each value of the first line of the table from Figure 3a with random number $R_1 = 11$. Thus, EXORing the value 00 of the first line and first column of the table from Figure 3a with the number 11 yields the value 11, which is now the element of the first line and first column of the table of Figure 3b. The remaining values of the first line of the table shown in Figure 3b are determined accordingly from the values of the first line of the table shown in Figure 3a and random number $R_1 = 11$. The table shown in Figure 3b could already be used as a disguised lookup table for processing secret data likewise disguised with random number $R_1 = 11$. The result would be the plaintext values to be read in line 2 of the table from Figure 3b.

One usually arranges the individual columns of a lookup table according to ascending input data x. A table determined by accordingly sorting the table in Figure 3b is shown in Figure 3c.

If the table according to Figure 3c is to be disguised further or yield as output values likewise disguised values rather than plaintext values, one applies a further EXOR operation with further random number R_2.

Figure 3d shows the result of applying said further EXOR operation. In said operation the elements of the second line of the table according to Figure 3c are each EXORed with random number $R_2 = 10$. The element in the second line and the first column of the table according to Figure 3d thus results from EXORing the element in the second line and first column of the table according to Figure 3c with random number $R_2 = 10$. The further elements of the second line of the table according to Figure 3d are formed accordingly. The first line of the table according to Figure 3d is adopted by Figure 3c unchanged.

With the table shown in Figure 3d one can determine likewise disguised output data from disguised input data. The thus determined disguised output data can be supplied to further operations for processing disguised data or one can determine plaintext data therefrom by EXORing with random number $R_2 = 10$.

Use of the table shown in Figure 3d makes it possible to perform nonlinear operations with disguised secret data and protect said secret data from unauthorized access. The security-relevant operations themselves are still also protected from un-

authorized access since differently disguised functions can be used at every execution of the operations and the security-relevant operations themselves cannot be inferred even if the disguised functions could be determined. After conversion to plaintext, however, both the original security-relevant operations and the operations performed with the aid of disguised functions yield identical results. For example, input value 00 yields output value 01 according to the table in Figure 3a. In order to check whether the disguised table shown in Figure 3d yields the same output value one must first EXOR input value 00 with random number R_1 = 11. As a result of said combination one obtains the value 11. According to the table from Figure 3d, input value 11 likewise yields output value 11. In order to determine the plaintext from said output value one must EXOR the output value with random number R_2 = 10. As a result of said combination one obtains the value 01 which exactly matches the value determined with the aid of the table shown in Figure 3a.

Disguising the security-relevant operations or the input values can be effected not only by EXORing but also by other suitable types of combination, for example modular addition. Furthermore, the invention is not limited to the application of nonlinear functions represented by means of lookup tables. One can also use any nonlinear and even linear functions for which a suitable disguised function can be determined.

Patent claims

1. A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that
   - the operation (h) is disguised before its execution,
   - the disguised operation (h_{R1}) is executed with disguised input data ($x \otimes R_1$), and
   - the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h_{R1}) with disguised input data ($x \otimes R_1$) yields output data (y) identical with the output data (y) determined upon execution of the undisguised operation (h) with undisguised input data (x).
2. A data carrier according to claim 1, characterized in that at least one random number (R_1) enters into the determination of the disguised operation (h_{R1}) and the disguised input data ($x \otimes R_1$).
3. A data carrier according to either of the above claims, characterized in that the determination of the disguised operation (h_{R1}) and the disguised input data ($x \otimes R_1$) is effected with the aid of EXOR operations.
4. A data carrier according to any of the above claims, characterized in that the disguised operation (h_{R1}) is permanently stored in the data carrier in advance.
5. A data carrier according to claim 4, characterized in that at least two disguised operations (h_{R1}, $h_{R1'}$) are permanently stored in the data carrier in advance and one of the stored disguised operations (h_{R1}, $h_{R1'}$) is selected randomly when a disguised operation is to be executed.
6. A data carrier according to any of claims 1 to 3, characterized in that the disguised operation (h_{R1}) is recalculated before its execution and the at least one random number (R_1) is redetermined for said calculation.

7. A data carrier according to any of the above claims, characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y).

8. A data carrier according to claim 7, characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1).

9. A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that
   - the operation (h) is disguised before its execution,
   - the disguised operation (h_{R1}) is executed with disguised input data ($x \otimes R_1$),
   - the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h_{R1R2}) with disguised input data ($x \otimes R_1$) yields output data ($y \otimes R_2$) which are disguised relative to the output data (y) determined upon execution of the undisguised operation (h) with undisguised input data (x), and
   - the undisguised output data (y) can be determined from the disguised output data ($y \otimes R_2$) with the aid of data (R_2) used for disguising the operation (h).

10. A data carrier according to claim 9, characterized in that at least one random number (R_1) enters into the determination of the disguised input data ($x \otimes R_1$) and at least two random numbers (R_1, R_2) enter into the determination of the disguised operations (h_{R1R2}).

11. A data carrier according to either of claims 9 and 10, characterized in that the determination of the disguised operation (h_{R1R2}) and the disguised input data ($x \otimes R_1$) is effected with the aid of EXOR operations.

12. A data carrier according to any of claims 9 to 11, characterized in that the disguised operation (h_{R1R2}) is permanently stored in the data carrier in advance.

13. A data carrier according to claim 12, characterized in that at least two disguised operations (h_{R1R2}, $h_{R1'R2'}$) are permanently stored in the data carrier in advance and one of the stored disguised operations (h_{R1R2}, $h_{R1'R2'}$) is selected randomly when a disguised operation is to be executed.

14. A data carrier according to claim 13, characterized in that the random numbers (R_1, R_2) for determining the first disguised operation (h_{R1R2}) are inverse to the random numbers (R_1', R_2') for determining the second disguised operation ($h_{R1'R2'}$) with respect to the combination used for determining the disguised operations (h_{R1R2}, $h_{R1'R2'}$).

15. A data carrier according to any of claims 9 to 11, characterized in that the disguised operation (h_{R1R2}) is recalculated before its execution and the random numbers (R_1, R_2) are redetermined for said calculation.

16. A data carrier according to any of claims 9 to 15, characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y).

17. A data carrier according to claim 16, characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1) and the disguising of the output data (y) contained in the table is effected by combination with the at least one further random number (R_2).

18. A data carrier according to any of the above claims, characterized in that the operation (h) is a nonlinear operation with respect to the combination used for disguising the operation (h).

Abstract

The invention relates to a data carrier having a semiconductor chip (5) with at least one memory. The memory contains an operating program that is able to perform at least one operation (h). In order to prevent unauthorized access to the data (x) processed with the operation (h), both said data and the operation (h) itself are disguised. The disguising of the data (x) and the operation (h) is coordinated such that the disguised operation (h_{R1R}, h_{R1R2}) generates either the output data (y) of the undisguised operation (h) or disguised output data ($y \otimes R_2$) from which the output data (y) can be determined.

FIG.1

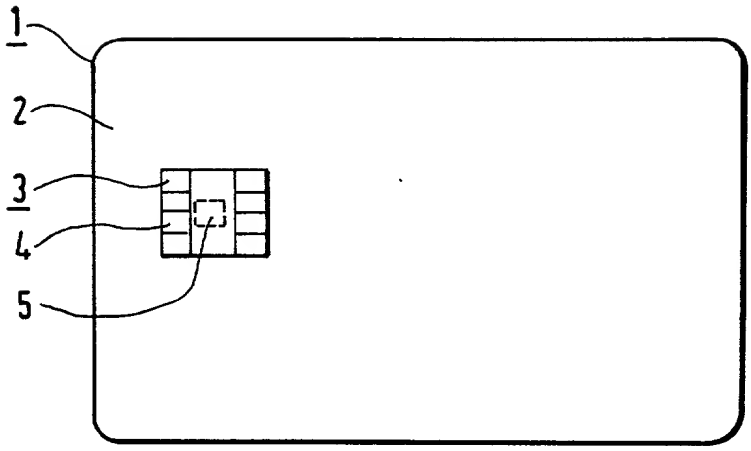

FIG.2

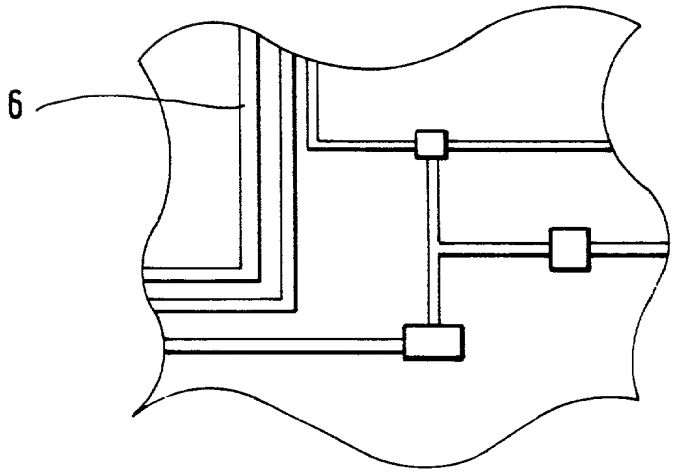

FIG. 3A

x	00	01	10	11
h(x)	01	11	10	00

FIG. 3B

x	11	10	01	00
$h_{R1}(x)$	01	11	10	00

FIG. 3C

x	00	01	10	11
$h_{R1}(x)$	00	10	11	01

FIG. 3D

x	00	01	10	11
$h_{R1\,R2}(x)$	10	00	01	11

ATTORNEY/DOCKET NO. **JEK/Vater**

23364
PATENT TRADEMARK OFFICE

DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention (Design, if applicable) entitled:
ACCESS-PROTECTED DATA CARRIER

the specification of which (check one):

☐ is attached hereto, or ☒ was filed on: **07 September 1999** as U.S. Application Number or PCT International Application Number: **(PCT/EP99/06580) 09/763,621**
and (if applicable) was amended on:

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56.* I hereby claim foreign priority benefits under *Title 35, United States Code §119* of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR FOREIGN APPLICATION(S)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No
198 41 676.8	Germany	11 September 1999	X	
		11 Sept 1998		

☐ Additional Priority Application(s) Listed on Following Page(s)

I HEREBY CLAIM THE BENEFIT UNDER TITLE 35 U.S. CODE §119(E) OF ANY U.S. PROVISIONAL APPLICATIONS LISTED BELOW.	
Application Number	Day/Month/Year Filed

☐ Additional Provisional Application(s) Listed on Following Page(s)

I hereby claim the benefit under *Title 35, United States Code, §120* of any United States application(s) or PCT international application(s) designating The United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of *Title 35, United States Code, §112*, I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1 56* which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Number	Filing Date	Status - Patented, Pending or Abandoned

☐ Additional US/PCT Priority Application(s) listed on Following Page(s)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under *section 1001 of title 18 of the United States Code* and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: I (We) hereby appoint as my (our) attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: J. Ernest Kenney, Reg. No. 19,179; Eugene Mar, Reg. No. 25,893; Richard E. Fichter, Reg. No. 26,382; Thomas J. Moore, Reg. No. 28,974; Joseph DeBenedictis, Reg. No. 28,502; Benjamin E. Urcia, Reg. No. 33,805; and

I(we) authorize my(our) attorneys to accept and follow instructions from **Klunker Schmitt-Nilson Hirsch** regarding any matter related to the preparation, examination, grant and maintenance of this application, any continuation, continuation-in-part or divisional based thereon, and any patent resulting therefrom, until I(we) or my(our) assigns withdraw this authorization in writing.

Send correspondence to: **BACON & THOMAS, PLLC**
625 Slaters Lane - 4th Floor
Alexandria, VA 22314-1176

Telephone Calls to: **J. Ernest Kenney (703) 683-0500**

FULL NAME OF FIRST OR SOLE INVENTOR	CITIZENSHIP
Harald VATER	**Germany**
RESIDENCE ADDRESS An den Schulgarten 23, D-35398 Giessen, Germany DEX	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 23. 3. 2001	SIGNATURE Harald Vater

☒ *See following page(s) for additional joint inventors.*

CONTINUATION OF DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

PRIOR FOREIGN APPLICATION(S) (35 USC §119)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No

PRIOR PROVISIONAL APPLICATIONS 35 U.S. CODE §119(E)	
Application Number	Day/Month/Year Filed

PRIOR U.S. OR PCT INTERNATIONAL APPLICATIONS (35 U.S. CODE §120)		
Application Number	Filing Date	Status - Patented, Pending or Abandoned

2-00

FULL NAME OF JOINT INVENTOR Hermann DREXLER	CITIZENSHIP Germany
RESIDENCE ADDRESS Oberlanderstrasse 5a, D-81371 Munchen, Germany DEX	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 2.4.2001	SIGNATURE [signature]

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
RESIDENCE ADDRESS	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
RESIDENCE ADDRESS	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
RESIDENCE ADDRESS	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

☐ *See following pages for additional joint inventors/priority applications.*